

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR UNITED STATES PATENT

FOR

**APPARATUS AND METHOD OF IMPLEMENTING MULTICAST
SECURITY BETWEEN MULTICAST DOMAINS**

Inventors:

Yunzhou Li

351 Pawtucket Boulevard Unit 7
Lowell, MA 01854

Billy C. Ng

1722 North Shore Drive
Revere, MA 02151

Jyothi Hayes

215 Stow Road
Harvard, MA 01451

Attorney Docket: 2204/198
(BA-442)

Attorneys:

BROMBERG & SUNSTEIN LLP
125 Summer Street
Boston, MA 02110
(617) 443-9292

APPARATUS AND METHOD OF IMPLEMENTING MULTICAST SECURITY BETWEEN MULTICAST DOMAINS

PRIORITY

This application claims priority from co-pending provisional U.S. Patent Application Serial Number 60/137,235, filed June 2, 1999, entitled "APPARATUS AND METHOD OF BRIDGING MULTICAST SECURITY BETWEEN MULTICAST DOMAINS" and bearing attorney docket number 2204/165, the disclosure of which is incorporated herein, in its entirety, by reference.

CROSS REFERENCE TO RELATED APPLICATIONS

This application is related to U.S. Patent Application Serial Number xx/xxx,xxx filed on even date herewith, entitled "APPARATUS AND METHOD OF MINIMIZING INTERNAL MULTICAST TRAFFIC" and bearing attorney docket number 2204/195, naming Yunzhou Li as inventor, the disclosure of which is incorporated herein, in its entirety, by reference.

FIELD OF THE INVENTION

The invention generally relates to networks and, more particularly, the invention relates to multicast transmissions across a computer network.

BACKGROUND OF THE INVENTION

Multicasting is a well-known method of transmitting information to selected groups of users across a network, such as the Internet. For example, the transmission of an E-mail message to a group of users, each user being listed on a mailing list, uses multicasting

principles. Video conferencing and teleconferencing also use multicasting principles and, accordingly, are often referred to as "multiconferencing."

Due to increased demand for uses utilizing multicasting principles, protocols such as the Internet Group Multicast Protocol ("IGMP") have been developed and refined to support multicasting over a Transmission Control Protocol/Internet Protocol ("TCP/IP") network, such as the Internet. The new protocols, such as IGMP, allow users to easily create and join multicasting sessions ("multicasts"). However, multicasts often transmit confidential information between multicast users ("members") during the multicast. Thus, a need exists for securing multicast transmissions.

However, because multicasting involves groups of users, securing multicast transmissions raises the issue of scalability. In response to this issue, it is recognized that it would be more scalable to allow the use of multiple, independent group security associations. In one such scheme, each packet is decrypted, and then re-encrypted, subgroup to subgroup, until the packet reaches the destination member. However, as a result of the decryption and re-encryption from subgroup to subgroup, the multicast transmission incurs latency. In addition, a problem arises when a multicast transmission is sent from a data originator that only allows an authorized agent or broker to translate the multicast transmission.

In another scheme, a multicast network is partitioned into hierarchical multiple security domains. In this scheme, however, a multicast transmission cannot be translated across horizontal domains.

SUMMARY OF THE INVENTION

In accordance with one aspect of the invention, an apparatus and method of implementing multicast security in a given multicast domain, the given multicast domain having one or more network devices, receives multicast traffic that is encrypted with a global key, the global key being available to the given multicast domain and one or more other multicast domains, decrypts the received multicast traffic with the global key to produce decrypted multicast traffic, encrypts the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available to the given multicast

domain, and forwards the local encrypted multicast traffic to the one or more network devices in the given multicast domain. In a further embodiment, the apparatus and method of implementing multicast security in a given multicast domain first receives a global key message that identifies the global key.

10 In an alternate embodiment of the invention, the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain. In a further alternate embodiment of the invention, the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message. In a still further alternate embodiment of the invention, the local key is only available to the given multicast domain.

15 In accordance with another aspect of the invention, a method of implementing multicast security in a given multicast domain receives multicast traffic that is encrypted with a global key, the global key being available to the given multicast domain and one or more other multicast domains, determines that the given multicast domain contains no network devices interested in the received multicast traffic, and sends a terminate message to no longer forward the received multicast traffic to the given multicast domain. In a further
20 embodiment of the invention, the method of implementing multicast security in a given multicast domain first receives a global key message that identifies the global key.

25 In a still further embodiment of the invention, the method of implementing multicast security in a given multicast domain determines, after having sent the terminate message, that the given multicast domain contains one or more network devices interested in the received multicast traffic and sends a resume message to once again forward the received multicast traffic to the given multicast domain.

30 In accordance with a further aspect of the invention, an apparatus and method of implementing multicast security in a network encrypts multicast traffic with a global key, the global key being available to a given multicast domain and one or more other multicast domains, forwards the global encrypted multicast traffic to the given multicast domain, receives the global encrypted multicast traffic at the given multicast domain, decrypts at the given multicast domain the global encrypted multicast traffic with the global key to produce decrypted multicast traffic, encrypts at the given multicast domain the decrypted multicast

traffic with a local key to produce local encrypted multicast traffic, the local key being available to the given multicast domain, and forwards the local encrypted multicast traffic to one or more network devices in the given multicast domain. In a further embodiment of the invention, the apparatus and method of implementing multicast security in a network first receives at the given multicast domain a global key message that identifies the global key.

10 In an alternate embodiment of the invention, the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain. In a further alternate embodiment of the invention, the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message. In a still further alternate embodiment of the invention, the local key is only available to the given multicast domain.

15 In accordance with a still further aspect of the invention, a method of implementing multicast security in a given multicast domain receives multicast traffic, constructs, in response to the received multicast traffic, an information message that alerts other multicast domains of the security capabilities of the given multicast domain, and forwards the information message to at least one other multicast domain. In a further embodiment of the invention, the information message is a part of a multicast protocol message. In a still further embodiment of the invention, one or more bits in one or more fields of the multicast protocol message are set to alert other multicast domains of the security capabilities of the given multicast domain.

20 In other embodiments of the invention, the given multicast domain is a protocol independent multicast domain or, in the alternative, the given multicast domain is a group of contiguous protocol independent multicast domains. In a still other embodiment of the invention, the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

25
30

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects and advantages of the invention will be appreciated more fully from the following further description thereof with reference to the accompanying drawings wherein:

Figure 1 shows an exemplary process for implementing the invention in a particular
10 multicast domain.

Figure 2 schematically shows an exemplary Multicast Source Discovery Protocol ("MSDP") backbone, in which various embodiments of the invention may be implemented.

Figure 3 shows an exemplary process for implementing the invention between
15 multicast domains in the exemplary MSDP backbone shown in Figure 2.

Figure 4 shows an exemplary process for implementing the invention between
20 multicast domains in the exemplary MSDP backbone shown in Figure 2 using DVMRP for support.

Figure 5 shows an exemplary process for implementing the invention between
25 multicast domains in the exemplary MSDP backbone shown in Figure 2 using BGMP for support.

Figure 6 shows a block diagram of an exemplary apparatus for implementing the
invention between multicast domains in the exemplary MSDP backbone shown in Figure 2.

Figure 7 shows an exemplary process for initial key distribution of a global group
specific key and local group specific keys for a particular multicast.

DETAILED DESCRIPTION OF THE INVENTION

In accordance with an embodiment of the invention, multicast security between
multicast domains, particularly Protocol Independent Multicast-Sparse Mode ("PIM-SM")
domains, is implemented through a Multicast Source Discovery Protocol ("MSDP") bridge.
30 A multicast protocol, such as Distance Vector Multicast Routing Protocol ("DVMRP"), runs
over the MSDP bridge to forward secure multicast traffic in the global key space. A security
broker in each interested multicast domain translates the multicast traffic from the MSDP
bridge to the local domain and forwards the multicast traffic in the local key space.

Figure 1 shows an exemplary process for implementing various embodiments of the invention in a particular multicast domain. The process begins at step 100, in which encrypted multicast traffic for a multicast group is received in a particular multicast domain. The multicast traffic has been previously encrypted with a symmetrical encryption key that is available to the multicast domain. The key is also available to one or more other multicast domains. Thus, for reference purposes, the key is referred to as a "global group specific key." The process continues at step 105, in which the encrypted multicast traffic is decrypted with the global group specific key. At step 110, the multicast traffic is re-encrypted. At this step, the multicast traffic is encrypted using a local group specific key, i.e., a key available to the particular multicast domain, but not necessarily available to other multicast domains. In alternate embodiments, the local group specific key may only be available to the particular multicast domain. At step 115, the re-encrypted multicast traffic is forwarded to one or more network devices in the particular multicast domain. Ultimately, the network devices forward the multicast traffic to the receivers (or users) of the multicast (not shown). The receivers (or users) of a multicast are referred to as "members" of a multicast. Members of a multicast who have acquired a local group specific key for the multicast in their multicast domain are referred to as secure members.

In another embodiment of the invention, the re-encrypted multicast traffic is forwarded to all of the network devices in the particular multicast domain (not shown). In the alternative, the re-encrypted multicast traffic is forwarded to a subset of the network devices in the particular multicast domain (not shown).

Figure 2 schematically shows an exemplary MSDP backbone, MSDP backbone 200, in which various embodiments of the invention may be implemented. MSDP backbone 200 includes five multicast domains--domain 210, domain 220, domain 230, domain 240 and domain 250. Domain 210 is a remote Protocol Independent Multicast ("PIM") domain. It includes MSDP Server 212, source security broker 214, and source 205. MSDP Server 212 is a network device configured to receive multicast messages sent to domain 210. For example, MSDP Server 212 may be configured to receive all multicast messages sent to domain 210. Source security broker 214 is a network device responsible for multicasts in a particular range of multicast addresses, referred to as the Rendezvous Point ("RP") for the particular

multicasts. In remote domain 210, source security broker 214 is the RP for the multicast being sent from source 205.

Domains 220, 230, 240, and 250 are local PIM domains. Domain 220 includes MSDP Server 222. Domain 230 includes MSDP Server 232 and member security broker 234. Domain 240 includes MSDP Server 242 and member security broker 244. Domain 250 includes MSDP Server 252 and member security broker 254. Similar to source security broker 214, the member security brokers are the RPs in their respective multicast domains for the multicast being sent from source 205. For example, member security broker 234 is the RP in local domain 230 for the multicast being sent from source 205.

Connectors 20, 22, 24, 26, and 28 show the peering relationship between the MSDP Servers. For example, MSDP Server 212 in remote domain 210 peers, in an external peering relationship, with MSDP Server 222 in local domain 220. An external peering relationship occurs between MSDP Servers in neighboring PIM domains or, if the neighboring PIM domain does not contain a MSDP Server, between the MSDP Server and a RP in the neighboring domain. In one embodiment, TCP connections are set up and GRE tunnels are configured over connectors 20, 22, 24, 26, and 28.

In contrast, the member security brokers in the local domains peer with their respective MSDP Servers in an internal peering relationship in the multicast domain. An internal peering relationship occurs between a MSDP Server in the multicast domain and the network device in the multicast domain responsible for particular multicasts, *i.e.*, the RPs. For example, MSDP Server 242 in local domain 240 peers internally with member security broker 244.

In MSDP backbone 200, security brokers 214, 234, 244, and 254 are the RPs in their respective multicast domains for the multicast being sent from source 205.

In an alternate embodiment, MSDP backbone 200 may also include a group (or groups) of contiguous PIM domains (not shown). In this configuration, the security broker for the group of contiguous PIM domains (whether a source security broker or member security broker) is the root of the shared tree for the group.

Figures 3a-3b show an exemplary process for implementing various embodiments of the invention between multicast domains in MSDP backbone 200. The process begins at step

300, in which source 205 encrypts the multicast traffic using a local group specific key for the multicast for remote domain 210 (referred to as "K210"). The process continues at step 303, in which source 205 forwards the encrypted multicast traffic to source security broker 214. At step 306, source security broker 214 forwards the encrypted multicast traffic to the secure members in remote domain 210. As discussed below in reference to Figure 7 (step 735),
10 secure members of the multicast in remote domain 210 have previously received "K210" (the local group specific key for the multicast for remote domain 210) from source security broker 214. Thus, because source 205 encrypted the multicast traffic using "K210", source security broker 214 can forward the encrypted multicast traffic to the secure members in remote domain 210 without the need for security translation.

15 The process continues at step 309, in which source security broker 214 decrypts the encrypted multicast traffic using "K210" (the local group specific key for the multicast for remote domain 210) and, at step 312, re-encrypts the decrypted multicast traffic using a global group specific key for the multicast being sent from source 205 (referred to as "K200"). At step 315, source security broker 214 forwards the re-encrypted multicast traffic
20 to MSDP Server 212 in remote domain 210.

MSDP Server 212, at step 318, externally forwards the re-encrypted multicast traffic to MSDP Server 222 in local domain 220 through a GRE tunnel configured over connector 160. At step 321, MSDP Server 222 externally forwards the re-encrypted multicast traffic to MSDP Server 232 in local domain 230 over connector 162 and to MSDP Server 252 in local
25 domain 250 over connector 168. MSDP Server 222 in local domain 220 does not internally forward the re-encrypted multicast traffic because local domain 220 does not contain a member security broker.

The process now continues at local domain 230. At step 324, MSDP Server 232 in local domain 230 internally forwards the re-encrypted multicast traffic to member security
30 broker 234 and, at step 327, externally forwards the re-encrypted multicast traffic to MSDP Server 242 in local domain 240 via connector 164. Member security broker 234, at step 330, decrypts the re-encrypted multicast traffic using "K200" (the global group specific key for the multicast being sent from source 205) and, at step 333, re-re-encrypts the multicast traffic using a local group specific key for the multicast for local domain 230 (referred to as

“K230”). At step 336, member security broker 234 forwards the re-re-encrypted multicast traffic to secure members in local domain 230. As discussed below in reference to Figure 7 (step 740), secure members of the multicast in local domain 230 have previously received “K230” from member security broker 234.

The process now continues at local domain 240. At step 339, MSDP Server 242 internally forwards the re-encrypted multicast traffic to member security broker 244 and, at step 342, externally forwards the re-encrypted multicast traffic to MSDP Server 252 in local domain 250 via connector 166. Member security broker 244, at step 345, decrypts the re-encrypted multicast traffic using “K200” (the global group specific key for the multicast being sent from source 205) and, at step 348, re-re-encrypts the multicast traffic using a local group specific key for the multicast for local domain 240 (referred to as “K240”). At step 351, member security broker 244 forwards the re-re-encrypted multicast traffic to secure members in local domain 240. As discussed below in reference to Figure 7 (step 745), secure members of the multicast in local domain 240 have previously received “K240” from member security broker 244.

The process now continues at local domain 250. As discussed at steps 321 and 342 above, MSDP Server 252 has received the re-encrypted multicast traffic from both MSDP Server 222 in local domain 220 (step 321) and MSDP Server 242 in local domain 240 (step 342). Thus, at step 354, MSDP Server 252 first determines that the next hop to source 205 is MSDP Server 222 in local domain 220. Accordingly, at step 357, MSDP Server 252 drops the re-encrypted multicast traffic from MSDP Server 242 in local domain 240 and, at step 360, forwards a message to MSDP Server 242 to no longer forward the re-encrypted multicast traffic to it. MSDP Server 252 then, at step 363, internally forwards the re-encrypted multicast traffic to member security broker 254 and, at step 366, externally forwards the re-encrypted multicast traffic to MSDP Server 242 in local domain 240. At step 369, member security broker 254 decrypts the re-encrypted multicast traffic using “K200” (the global group specific key for the multicast being sent from source 205) and, at step 372, forwards the decrypted multicast traffic to members in local domain 250.

The process now moves back to local domain 240. As discussed above at steps 327 and 365, MSDP Server 242 has received the re-encrypted multicast traffic from both MSDP

Server 232 in local domain 230 (step 327) and MSDP Server 252 in local domain 250 (step 365). Thus, at step 375, MSDP Server 242 determines that the next hop to source 205 is MSDP Server 232. Accordingly, at step 378, MSDP Server 242 drops the re-encrypted multicast traffic from MSDP Server 252 in local domain 250 and, at step 381, forwards a message to MSDP Server 252 to no longer forward the re-encrypted multicast traffic to it.

10 In other embodiments of the invention, the process for implementing multicast security between multicast domains is executed in accordance with a multicast protocol. At present, DVMRP is one of the various multicast protocols to run because DVMRP has its own routing. With Multicast Broader Gateway Protocol ("MBGP") routing in place, Border Gateway Multicast Protocol ("BGMP") is another multicast protocol to run. In addition, the
15 MSDP backbone may be partitioned into numerous multicast routing domains, each running a different multicast protocol.

Figure 4 shows an exemplary process for implementing various embodiments of the invention between multicast domains in MSDP backbone 200 using DVMRP for support. The process begins at step 400, in which source 205 encrypts the multicast traffic using
20 "K210" (the local group specific key for the multicast for remote domain 210). The process continues at step 405, in which source 205 forwards the encrypted multicast traffic to source security broker 214 through a PIM Register message. At step 410, source security broker 214 deregisters the encrypted multicast traffic and forwards it to the secure members in remote domain 210 without security translation. As discussed below in reference to Figure 7 (step
25 735), secure members of the multicast in remote domain 210 have previously received "K210" (the local group specific key for the multicast for remote domain 210) from source security broker 214. Thus, because source 205 encrypted the multicast traffic using "K210", source security broker 214 can forward the encrypted multicast traffic to the secure members in remote domain 210 without the need for security translation.

30 At step 415, source security broker 214 decrypts the encrypted multicast traffic using "K210" (the local group specific key for the multicast for remote domain 210) and, at step 420, re-encrypts the multicast traffic using "K200" (the global group specific key for the multicast being sent from source 205). Source security broker 214 then forwards, at step 425, the re-encrypted multicast traffic over MSDP backbone 200 in accordance with DVMRP.

The process now continues at, for example, local domain 230. At step 430, member security broker 234 first determines whether local domain 230 contains any secure members for the multicast being sent from source 205. In other words, member security broker 234 determines whether any members in local domain 230 have acquired "K230" (the local group specific key for the multicast for local domain 230). If yes, then member security broker 234, at step 435, decrypts the re-encrypted multicast traffic using "K200" (the global group specific key for the multicast being sent from source 205) and, at step 440, re-re-encrypts the multicast traffic using "K230" (the local group specific key for the multicast for the local domain 230). At step 445, member security broker 234 forwards the re-re-encrypted multicast traffic to the secure members in local domain 230. If no, then member security broker 234, at step 450, triggers a DVMRP prune towards source security broker 214 over MSDP backbone 200.

If, at a later time, some domain members acquire the local group specific key for the domain (in other words, become secure members), then the security broker for the domain will trigger a DVMRP graft message toward the source security broker. For example, at step 450, member security broker 234 has determined that none of the members in local domain 230 are secure members. Accordingly, member security broker 234 has sent a DVMRP prune message towards source security broker 214 over MSDP backbone 200. Presently, member security broker 234 determines that one or more of the members in local domain 230 have now acquired "K230" (the local group specific key for the multicast for local domain 230), i.e., have become secure members (not shown). Accordingly, member security broker 234 sends a DVMRP graft message toward source security broker 214 (not shown). Source security broker 214 will, once again, forward re-encrypted multicast traffic toward member security broker 234 over MSDP backbone 200 (not shown).

Figure 5 shows an exemplary process for implementing various embodiments of the invention between multicast domains in MSDP backbone 200 using BGMP for support. The process begins at step 500, in which source 205 encrypts the multicast traffic using "K210" (the local group specific key for the multicast for remote domain 210). The process continues at step 505, in which source 205 forwards the encrypted multicast traffic to source security broker 214 through a PIM Register message. At step 510, source security broker 214

constructs a Source Active ("SA") message with a G-bit set in the reserved field and, at step 515, forwards the SA message to, for example, member security broker 234 in local domain 230.

The process now continues at local domain 230. At step 520, member security broker 234 first determines whether any of the members in local domain 230 are interested in the
10 multicast being sent from source 205. If yes, at step 525, member security broker 234 triggers a BGMP join towards source security broker 214. (The coding for the BGMP join is (SSB214, G).)

The process now moves back to remote domain 210. At step 530, source security
5 broker 214 decrypts the encrypted multicast traffic using "K210" (the local group specific key for the multicast for the remote domain 210) and, at step 535, re-encrypts the multicast traffic using "K200" (the global group specific key for the multicast being sent from source 205). At step 540, source security broker 214 forwards the re-encrypted multicast traffic to member security broker 234 in local domain 230.

The process now continues at local domain 230. At step 545, member security broker
20 234 decrypts the re-encrypted multicast traffic using "K200" (the global group specific key for the multicast being sent from source 205) and, at step 550, re-re-encrypts the multicast traffic using "K230" (the local group specific key for the multicast for local domain 230). At step 555, member security broker 234 forwards the re-re-encrypted multicast traffic to the secure members in local domain 230.

25 The BGMP join messages set up a branch of a source tree to the respective domain through the MSDP backbone. For example, the BGMP join (SSB214, G) message sent from member security broker 234 towards source security broker 214 set ups a branch of the source tree for local domain 230.

Figure 6 is a block diagram of an exemplary apparatus for implementing various
30 embodiments of the invention between multicast domains in MSDP backbone 200. The apparatus includes encryption module 600 and multicast directing module 610 in, for example, remote domain 210. In this exemplary embodiment of the invention, encryption module 600 encrypts multicast traffic using "K210" (the local group specific key for the multicast for remote domain 210). Multicast directing module 610 forwards the encrypted

multicast traffic to source security broker 214. It also forwards the encrypted multicast traffic to the secure members in remote domain 210, as well as to security module 615. Security module 615 decrypts the encrypted multicast traffic using "K210" (the local group specific key for the multicast for remote domain 210) and re-encrypts it using "K200" (the global group specific key for the multicast being sent from source 205). Multicast directing module 610 then forwards the re-encrypted multicast traffic over MSDP backbone 200 to, for example, multicast directing module 630 in local domain 230.

The apparatus further includes multicast directing module 630 and security module 635 in, for example, local domain 230. In this exemplary embodiment of the invention, multicast directing module 630 forwards the re-encrypted multicast traffic to security module 635. Security module 635 decrypts the re-encrypted multicast traffic using "K200" (the global group specific key for the multicast being sent from source 205) and re-re-encrypts the multicast traffic using "K230" (the local group specific key for the multicast for local domain 230). Multicast directing module 630 then forwards the re-re-encrypted multicast traffic to the secure members in local domain 230.

Figure 7 shows an exemplary process for initial key distribution of a global group specific key and local group specific keys for the multicast being sent from source 205. The process begins at step 700, in which a multicast is initiated at source 205. At step 705, the member security brokers in the local domains learn the identity of source security broker 214 through procedures familiar to those skilled in the art. In turn, at step 710, member security broker 234 in local domain 230 exchanges its local group specific key for the multicast (shown as "K230") with source security broker 214 through Internet Key Exchange ("IKE") protocol. Similarly, at steps 715 and 720, member security broker 244 in local domain 240 and member security broker 254 in local domain 250 exchange their local group specific keys for the multicast (shown as "K240" and "K250" respectively) with source security broker 214 through IKE protocol.

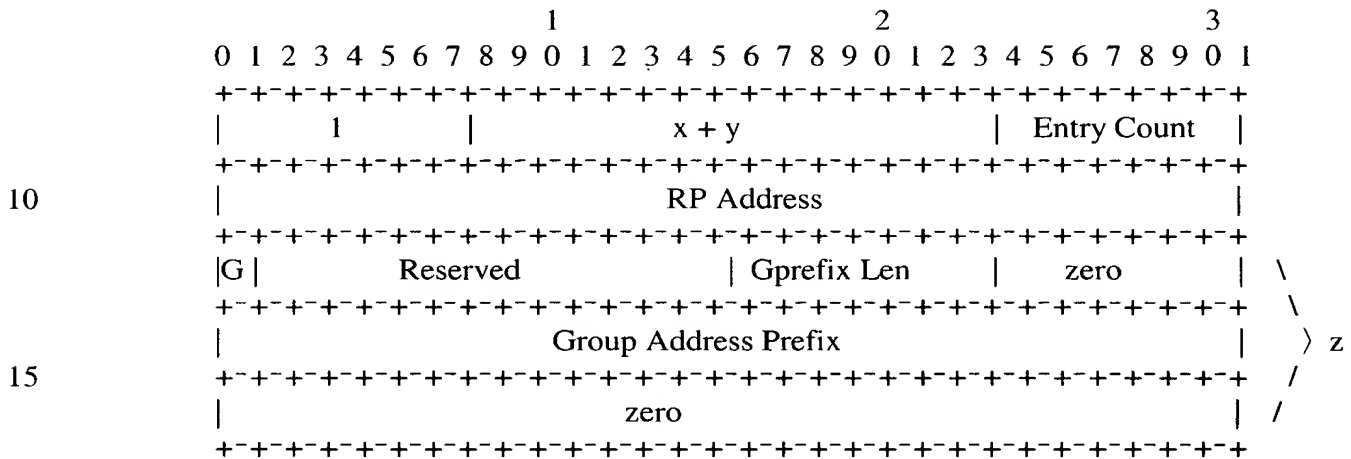
The process then continues at step 725, in which source security broker 214 encrypts the global group specific key for the multicast being sent from source 205 (shown as "K200") using, respectively, each member security brokers' local group specific key. It then forwards, respectively, at step 730, the encrypted global group specific key to the member security

brokers in the local domains. At step 735, source security broker 214 forwards the local group specific key for the multicast (shown as "K210") for remote domain 210 to source 205 and to receivers of the multicast in remote domain 210.

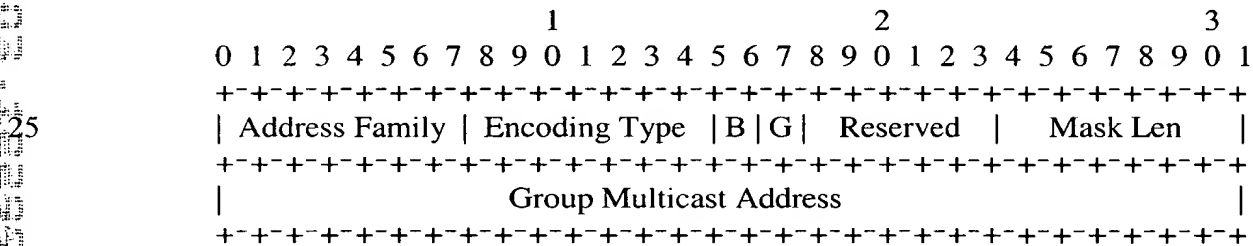
The member security brokers now continue the process of key distribution, as shown at steps 740 and 745. At step 740, member security broker 234 forwards "K230" (the local group specific key for the multicast for local domain 230) to members of the multicast in local domain 230. At step 745, member security broker 244 forwards "K240" (the local group specific key for the multicast for local domain 240) to members of the multicast in local domain 240. Because member security broker 254 forwards native data to members of the multicast in local domain 250, member security broker 254 does not need to forward a local group specific key to members of the multicast in local domain 250.

When multicast traffic is forwarded in accordance with the invention, it is referred to as being forwarded in MSDP bridge mode. In MSDP bridge mode, the PIM domains are separated without (S,G) joins in between. In addition, the multicast traffic is forwarded down a shared tree. In contrast, in native mode, the PIM domains learn of a multicast source through MSDP protocol, trigger (S,G) joins towards the source domain, and forward multicast traffic down the shortest path tree across the PIM domains.

A security broker explicitly informs other PIM-SM domains of its security broker configuration, i.e., decryption/encryption capabilities, through the MSDP bridge. In one embodiment, the security broker indicates its decryption/encryption capabilities through the use of a SA message. In particular, the security broker sets a G-bit in the reserved field of the SA message. However, because a SA message is used to indicate a secure group for all sources, when a security broker utilizes a SA message to explicitly inform other PIM-SM domains of its security broker configuration, the Sprefix Len and Source Address Prefix of the SA message is set to zero. The format is shown below:



When the SA message is received on a PIM-SM domain from the MSDP bridge, the security broker responsible for the secure multicast group correspondingly sets a G-bit in the reserved field of the encoded group address as follows:



30 The encoded group address is transmitted in the periodic Candidate-Rendezvous Point ("C-RP") advertisement. In turn, the bootstrap router carries the G-bit for the secure multicast group in each Bootstrap message. In this manner, all routers in the domain learn the identity of the security broker and the forwarding mode for a particular multicast group, and only join the shared tree.

35 For a particular multicast group, it is important that communication stay either constantly in MSDP bridge mode or constantly in native mode. There are two primary reasons for the need to maintain communications in either one or the other mode exclusively. First, the MSDP bridge is in a distinct secure key space from the PIM domains. Second, PIM domains on the shortest path tree will receive duplicate multicast traffic.

In order to enforce this behavior, each PIM router, when determining the G-bit is set for the security broker for a particular multicast group, should not trigger a (S,G) join. If the PIM router receives a (S,G) join from downstream, it should stop propagating the (S,G) join upstream towards the source. If there is already a (S,G) state in the PIM router for the particular group, the router should trigger a (*,G) join towards the relevant security broker. Or, the PIM router can remove the (S,G) prune. When multicast traffic arrives from the shared tree, the PIM router should trigger an (S,G) prune towards the S across the PIM domain.

The various embodiments of the invention may be implemented in any conventional computer programming language. For example, the various embodiments may be implemented in a procedural programming language (for example, "C") or an object-oriented programming language (for example, "C++"). The various embodiments of the invention may also be implemented as preprogrammed hardware elements (for example, application specific integrated circuits or digital processors), or other related components.

The various embodiments of the invention may be also implemented as a computer program product for use with a computer system. Such implementation may include a series of computer instructions fixed either on a tangible medium, such as a computer readable media (for example, a diskette, CD-ROM, ROM, or fixed disk), or transmittable to a computer system via a modem or other interface device, such as a communications adapter connected to a network over a medium. The medium may be either a tangible medium (for example, optical or analog communications lines) or a medium implemented with wireless techniques (for example, microwave, infrared or other transmission techniques). The series of computer instructions preferably embodies all or part of the functionality previously described herein with respect to the system. Those skilled in the art should appreciate that such computer instructions can be written in a number of programming languages for use with many computer architectures or operating systems. Furthermore, such instructions may be stored in any memory device, such as semiconductor, magnetic, optical or other memory devices, and may be transmitted using any communications technology, such as optical, infrared, microwave, or other transmission technologies. It is expected that such a computer program product may be distributed as a removable medium with accompanying printed or

electronic documentation (for example, shrink wrapped software), preloaded with a computer system (for example, on system ROM or fixed disk), or distributed from a server or electronic bulletin board over the network (for example, the Internet or World Wide Web).

Although various embodiments of the invention have been disclosed, it should be apparent to those skilled in the art that various changes and modifications can be made which will achieve some of the advantages of the invention without departing from the true scope of the invention. These and other obvious modifications are intended to be covered by the appended claims.

10

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198